KELLEY DRYE & WARREN LLP
A LIMITED LIABILITY PARTNERSHIP

WASHINGTON HARBOUR, SUITE 400
3050 K STREET, NW
WASHINGTON, D.C. 20007-5108

(202) 342-8400

FACSIMILE
(202) 342-8451
www.kelleydrye.com

NEW YORK, NY
TYSONS CORNER, VA
CHICAGO, IL
STAMFORD, CT
PARSIPPANY, NJ

BRUSSELS, BELGIUM

AFFILIATE OFFICES
MUMBAI, INDIA

October 31, 2006

VIA ECFS

Ms. Marlene Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Re: Notice of Ex Parte Presentation, CC Docket No. 96-115, RM-11277

Dear Ms. Salas:

XO Communications ("XO"), through its attorneys, respectfully submits this notice of *ex parte* presentation. On October 30, 2006, Lisa Youngers and Tokë Vandervoort from XO Communications and the undersigned, counsel to XO, met with Ian Dillner, Legal Advisor to Commissioner Tate to discuss the Notice of Proposed Rulemaking in the above-referenced proceeding. During the meeting, XO distributed the attached presentation, which summarizes the scope of its presentation; the content thereof is and XO's oral remarks were consistent with the comments and replies XO submitted previously in this proceeding.

Please contact either of us at 202-342-8400 if you have any questions regarding this filing.

Respectfully submitted,

John J. Heitmann
Jennifer M. Kashatus

cc: Ian Dillner (via email)

Attachment

XO Communications

Ex Parte Presentation – CC Docket No. 96-115, RM-11277

October 30, 2006

Summary

- There is no need to modify the FCC's existing CPNI rules – the FCC's current rules are sufficient to safeguard CPNI
- The FCC should not adopt any of EPIC's proposals
- The FCC also should not modify its rules pertaining to joint venture partners and independent contractors
- XO supports the adoption of a safe harbor

There is No Need to Modify the FCC's Current CPNI Rules

- Comments in this proceeding demonstrate an overwhelming carrier commitment to consumer privacy
- Comments in this proceeding also demonstrate that the risk to customer privacy is due to pretexting or other unlawful practices

The FCC Should Not Adopt Any of EPIC's Proposals

- Adoption of EPIC's proposals would cause carriers to incur significant costs without addressing the underlying problem: pretexting
- Customer-set passwords
  - Passwords are unworkable for business customers because the implementation of customer-set passwords on accounts with multiple administrators would be extremely costly and difficult to administer
  - Consumers do not want passwords
- Audit trails
  - FCC already has rejected the use of audit trails and there is no reason to revisit that decision
  - It would be extremely costly and burdensome for carriers to change or modify their databases to be able to implement audit trails

The FCC Should Not Adopt Any of EPIC's Proposals (cont.)

- Encryption
  - Unnecessary if a carrier maintains appropriate CPNI safeguards
  - Unworkable – the carrier would need to unencrypt the data each time it needed to access the data
  - Once the carrier unencrypts the data (for example, for billing purposes), the data is now available in a written unencrypted format outside of the carrier's system, thus negating the benefits of encrypting the data
  - Prohibitively costly and nearly impossible for to implement an encryption system – would require complete replacement of carrier billing practices
- CPNI Breach Notification
  - FCC should not require carriers to notify customers each time a breach has occurred
  - Not all CPNI breaches result in the misuse of data
  - Puts an undue burden on carriers; carriers may not have knowledge that a breach has occurred
  - If a security breach has resulted in the breach of personally identifiable information (such as social security number or credit card number) and carriers have knowledge of the breach, then carriers already are required to notify consumers that a breach has occurred under various federal and state statutes
  - If the FCC implements a breach notification rule, then it must limit breach notification duties to when carriers have knowledge that the customer's own personal and credit information has been compromised; carriers should not be required to notify customers after each release of CPNI

The FCC Should Not Modify Carrier Obligations with Regard to Joint Venture Partners and Independent Contractors

- There is no evidence that fraudulent access to records is due to joint venture partners or independent contractors
- Modifying the rules pertaining to independent contractors and joint venture partners would have an adverse impact on carrier operations by shutting down independent sales channels
- Modifying the rules would violate the First Amendment of the U.S. Constitution

XO Supports Adoption of a Safe Harbor

- XO supports adoption of a safe harbor based on best practices
  - XO supports the following safe harbor components:
    - Carriers must develop internal written procedures to protect CPNI
    - Carriers must conduct training regarding those procedures and the protection of CPNI
    - Carriers must develop internal standards for customer authentication
    - Carriers must file CPNI certifications with the FCC annually
    - Carriers must not use social security numbers for customer authentication
  - XO does not support inclusion of the following in any safe harbor:
    - Mandatory password protection for call center inquiries
    - Optional password protection for call center inquiries, unless limited to residential accounts
    - Customer notification of unauthorized access/disclosure of CPNI

Additional Considerations

- XO supports COMPTEL's request that the FCC affirmatively prohibit language in commercial agreements that would require CLECs to relinquish their control over customer CPNI
  - Contract provisions proposed in AT&T commercial agreements interfere with a CLEC's ability to protect its customer's CPNI
  - FCC should confirm that language in AT&T's (or any other commercial agreement) that hampers a carrier's ability to protect its customers' CPNI would be deemed unenforceable
- FCC should not apply CPNI rules to ISPs or information services
  - Doing so is not supported by section 222, which applies solely to information derived from "telecommunications services"
  - Applying CPNI requirements to information services is not necessary; EPIC is concerned about the release of telephone call records, and has not demonstrated any basis for applying CPNI requirements to ISPs or information services